MERTON COLLEGE IT SOFTWARE INSTALLATION POLICY

1. Approval and binding effect

1.1. The following Policy was **approved** by the Governing Body of Merton College ("the College") on 19 June 2023.

1.2. Any amendments to this Policy require the Governing Body's approval.

1.3. This Policy **must** be reviewed **annually** to ensure that any new developments are covered and protected.

1.4. All members of the College, all employees of the College, all departments within the College, and all other Users (as defined below) are bound by this Policy and are required to comply with it. For the avoidance of doubt any reference to employees or staff shall include permanent, temporary, contract and other support staff as applicable ; and "members" includes both Fellows and Junior Members.

1.5. The College regards breach of this Policy as a serious matter which may result in disciplinary action.

2. Definitions

2.1. "DPO" means the College's Data Protection Officer.

2.2. "Users" are Fellows, employees, students, consultants, contractors, agents and other authorised users accessing Merton College IT systems and applications.

2.3. 'MUST' and 'SHALL' mean that the item is an absolute requirement.

'MUST NOT' and 'SHALL NOT' mean that the item is absolutely prohibited.

'SHOULD' means that there may exist valid reasons in particular circumstances not to comply with a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

'SHOULD NOT' means that there may exist valid reasons in particular circumstances when particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

3. Scope and Purpose

3.1. Installation of unauthorised computer programs and software, including files downloaded and accessed on the Internet, can easily and quickly introduce serious, fast-spreading security vulnerabilities. Unauthorised software programs, even those seemingly provided by reputable vendors and trusted companies, can introduce viruses and Trojan programs that aid hackers' attempts to illegally obtain sensitive, proprietary and confidential data. Protecting the College's computers, systems, data and communications from unauthorised access and guarding against data loss is of

paramount importance; adherence to the following this Policy serves a critical role in the process.

3.2. This Policy applies to all computers or other devices which are connected to any College-provided system or network and are not self-managed. A computer or other device is self-managed if it has not been configured by the College's IT Department or is not automatically configured by a service provided by the College's IT Department. A computer or other device which has been purchased for a Fellow by the College from the Fellow's research allowance is usually self-managed. Users who have self-managed computers or other devices are responsible for configuring them as strongly and safely as practically possible.

3.3. This Policy outlines the approach of Merton College to IT software installation and provides the guiding principles and responsibilities to ensure the College's security objectives are met. It is intended to provide a single point of access for all Users who require information and guidance on this subject.

3.4. This Policy's purpose is to ensure every User agrees to abide by, specific guidelines for software, program and application installation and use on College-provided computers, systems and networks.

3.5. All use of the College's user accounts, desktop computers, laptop, servers, Internet and messaging services must conform to the guidelines presented in this Policy.

4. Policy

4.1. The College's IT Department tests and approves the use of specific software programs and applications only, including updates and patches to existing installed applications.

4.2. Software programs, applications and updates on all College systems and for those Users requiring those programs and applications **must** be approved and installed by the College's IT Department.

4.3. Employees and other Users **must** obtain written approval from the IT Department prior to requesting any unauthorised software or using any unapproved application on any College-provided equipment or systems.

4.4. Unauthorised applications **must not** be installed and used.

4.5. The College provides software programs and applications to increase productivity, enabling electronic communications and transacting business. Software programs and applications are provided as required to employees, contractors, temporary workers, volunteers and other authorised agents only to perform and fulfil job responsibilities. Software programs and applications are neither provided nor supported for non-business activities; the College's software programs and applications **must not** be used for personal activities.

4.6. The College's computer systems, networks and information technology services are provided to fulfil job tasks and responsibilities. The College places a priority on ensuring all installed software and applications are properly tested and licensed. Users

must not install software programs and applications, including software purchased for personal use.

4.7. Users **must not** download, install, copy, access, execute or otherwise employ any of the following:

- Illegal software or programs
- Unlicensed applications
- Unapproved or unlicensed operating systems
- Pirated software
- Software purchased for personal or home use.

4.8. The College provides IT software applications and programs as productivity enhancement tools. All College-provided software and licences remain the College's property.

4.8.1. If requested, users **must** surrender in a timely manner software licences, software media and other software and application materials provided by the College and discontinue their use.

4.8.2. Users **must not** make illegal copies of software, applications or programs.

5. Implementation and review

5.1. All Heads of Department **must** ensure that their staff are aware of this Policy. This should be undertaken as part of induction and supervision.

5.2. The DPO in co-operation with the Finance Bursar, the Sub-Warden, and the Senior Tutor **must** ensure that the Fellows and Junior Members of the College are aware of these Regulations and their requirements.

5.3. This Policy **shall** be reviewed and updated annually by the Finance Bursar and the DPO and approved by the Governing Body after review by the Finance Committee and the Statutes and Bylaws Committee

6. Useful Contacts

Data Protection Officer:	dpo@merton.ox.ac.uk 01865 276310 (College Lodge)
IT Department:	it-support@merton.ox.ac.uk 01865 276310 (College Lodge)
Head of IT:	head.of.it@merton.ox.ac.uk 01865 276310 (College Lodge)